(U//FOUO) OPEN SOURCE INTELLIGENCE REPORT (OSIR)

DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INTELLIGENCE AND ANALYSIS
OPEN SOURCE INTELLIGENCE REPORT
NOT FINALLY EVALUATED INTELLIGENCE

(U//FOUO) WARNING: THIS IS AN INFORMATION REPORT THAT CONTAINS RAW UNEVALUATED INFORMATION. THIS REPORT IS UNCLASSIFIED//FOR OFFICIAL USE ONLY.

(U//FOUO) This information is provided for intelligence and lead purposes only. This information may not be used as the basis for any U.S. legal process, including but not limited to: presentation to any U.S. Grand/Petit juries or administrative bodies; incorporation into affidavits or other documents relating to subpoenas, search, electronic surveillance, or arrest warrants; and/or as evidence in criminal prosecutions without the prior written authorization of DHS Headquarters.

(U//FOUO) SERIAL: OSIR-04001-0270-23

(U//FOUO) SUBJECT: Pro-Russian hacker group, Killnet, announced a distributed denial of service campaign against '50 hospitals' across '50 states of America'.

(U//FOUO) SUMMARY: Pro-Russian hacker group, Killnet, announced an "L7" distributed denial of service (DDoS) attack on "50 hospitals" across "50 states of America". The announcement included a list of domains and subdomains of healthcare and medical institutions located across 47 U.S. states and the District of Columbia. As of 2 February 2023, 41 of the 48 targeted domains and subdomains were accessible.

(U//FOUO) DATE OF ACQUISITION: 2/2/2023

(U//FOUO) ACQUISITION CODE: DD001

(U//FOUO) U.S. PERSONS INFORMATION (Y/N): NO

(U//FOUO) REQUIREMENT: 90261508; EEI-95149, EEI-95153, EEI-95154; 902651366; EEI-94641; 902652289; EEI-99235

(U//FOUO) TOPIC: DHS-IA-CYB.1, DHS-IA-CYB.3; HSEC-1.1, HSEC-1.2, HSEC-1.3, HSEC-1.5, HSEC-1.6, HSEC-1.8, HSEC-1.10

(U//FOUO) COUNTRY OR NONSTATE ENTITY: USA, RUS

(U//FOUO) DATE OF INFORMATION: 2/1/2023

(U//FOUO) SOURCE NUMBER: DHS-04001-03649

(U//FOUO) SOURCE DESCRIPTION: Operators of the public instant messaging channel for the pro-Russian hacker group, Killnet, with direct access to the information. Source regularly posts pro-Russian narratives in addition to claims of engaging in malicious cyber activities including Distributed Denial of Service (DDoS) attacks against the United States, Ukraine, and other countries which support Ukraine. The group claimed in September 2022, they are currently working with 14 other "Russian hacker groups" including, Anonymous Russia. The founder of Killnet is a Russian hacker operating under the pseudonym, KillMilk, who claimed in a 14 October 2022 post the group was receiving financial aid from an organization known as Solaris. KillMilk referred to Solaris as "the administration of which keeps the shadow market of the Russian Federation". Source's information has been evaluated and deemed credible.

(U//FOUO) SOURCE CONTEXT: An instant messaging channel operated by the hacker group KillNet. The channel primarily discusses pro-Russian topics relating to the Russia-Ukraine conflict. Content is primarily in the Russian language. KillNet also uses the channel to post the results of Distributed Denial of Service attacks and other cyber types of operations against Ukrainian, U.S., and NATO organizations.

(U//FOUO) TEXT:
1. (U//FOUO) On 1 February 2023, Killnet published two posts to their instant messaging channel stating, "ATTENTIONS TO TEAMS THAT JOIN OUR MISSION...L7 strike to everyone on 50 hospital targets - 50 states of America". Killnet included a list of 48 domains and subdomains associated with 48 identified U.S. healthcare and medical institutions located across 47 U.S. states and the District of Columbia. As proof of the attacks, Killnet provided links to the website monitoring tool, Check-Host, which showed all sites were inaccessible between 10:21 EST and 13:47 EST on 31 January 2023. In a subsequent post, Killnet called on, "all hack-teams, loners and anyone who has stressors, botnets, c2 panels, servers" to contact the administrator of Killnet's forum, Infinity, via the administrator's instant messaging channel. The three posts received 20.4K, 21.8K, and 5.4K respectively, as of 2 February 2023.

2. (U//FOUO) As of 2 February 2023 at 12:30 EST, 41 of the 48 affected domains and subdomains of the targeted U.S. healthcare and medical institutions were accessible. The locations and accessibility

of the identified U.S. healthcare and medical institutions' targeted domains and subdomains include:
-- [USPER 1] located in Anchorage, Alaska and accessible as of 2 February 2023.
-- [USPER 2] located in Phoenix, Arizona and accessible as of 2 February 2023.
-- [USPER 3] located in North Little Rock, Arkansas and accessible as of 2 February 2023.
-- [USPER 4] located in Broomfield, Colorado and accessible as of 2 February 2023 (Collector Comment: Killnet listed USPER 4's domain twice as the only targeted institution in California and Colorado.)
-- [USPER 5] located in Derby, Connecticut and accessible as of 2 February 2023.
-- [USPER 6] located in Newark, Delaware and accessible as of 2 February 2023.
-- [USPER 7] located in Fort Myers, Florida and accessible as of 2 February 2023.
-- [USPER 8] located in Lawrenceville, Georgia and inaccessible as of 2 February 2023 (Collector Comment: Attempts to connect to USPER 8's front-facing website returned "Error 20 - TCP Connection timeout)".
-- [USPER 9] located in Honolulu, Hawaii and accessible as of 2 February 2023.
-- [USPER 10] located in St. Maries, Idaho and accessible as of 2 February 2023.
-- [USPER 11] located in Chicago, Illinois and accessible as of 2 February 2023.
-- [USPER 12] located in La Porte, Indiana and accessible as of 2 February 2023.
-- [USPER 13] located in Iowa City, Iowa and accessible as of 2 February 2023.
-- [USPER 14] located in Belleville, Kansas and accessible as of 2 February 2023.
-- [USPER 15] located in Georgetown, Kentucky and accessible as of 2 February 2023.
-- [USPER 16] located in Baton Rouge, Louisiana and accessible as of 2 February 2023 (Collector Comment: Pro-Russian hacker group and affiliate of Killnet, Anonymous Russia, also targeted USPER 16 on 30 January 2023 with a DDoS attack).
-- [USPER 17] located in Brunswick, Maine and accessible as of 2 February 2023
-- [USPER 18] located in Silver Spring, Maryland and accessible as of 2 February 2023.
-- [USPER 19] located in Boston, Massachusetts and inaccessible as of 2 February 2023.
-- [USPER 20] located in Wyoming, Michigan and accessible as of 2 February 2023.
-- [USPER 21] located in Grand Rapids, Minnesota and accessible as of

2 February 2023.
-- [USPER 22] located in St. Marks, Mississippi and accessible as of 2 February 2023.
-- [USPER 23] located in Houston, Missouri and accessible as of 2 February 2023.
-- [USPER 24] located in Kalispell, Montana and accessible as of 2 February 2023.
-- [USPER 25] located in Omaha, Nebraska and accessible as of 2 February 2023.
-- [USPER 26] located in Boulder City, Nevada and accessible as of 2 February 2023 (Collector Comment: Pro-Russian hacker group and affiliate of Killnet, Anonymous Russia, also targeted USPER 26 on 30 January 2023 with a DDoS attack).
-- [USPER 27] located in Exeter, New Hampshire and inaccessible as of 2 February 2023.
-- [USPER 28] located in Secaucus, New Jersey and accessible as of 2 February 2023.
-- [USPER 29] located in Albuquerque, New Mexico and inaccessible as of 2 February 2023 (Collector Comment: Attempts to connect to USPER 29's front-facing website returned an "Account Suspended" error for the URL).
-- [USPER 30] located in Bronx, New York and accessible as of 2 February 2023.
-- [USPER 31] located in Raleigh, North Carolina and accessible, as of 2 February 2023.
-- [USPER 32] located in Minot, North Dakota and inaccessible as of 2 February 2023.
-- [USPER 33] located in Columbus, Ohio and inaccessible as of 2 February 2023.
-- [USPER 34] located in Oklahoma City, Oklahoma and accessible as of 2 February 2023.
-- [USPER 35] located in Coos Bay, Oregon and accessible as of 2 February 2023.
-- [USPER 36] located in Johnstown, Pennsylvania and inaccessible as of 2 February 2023.
-- [USPER 37] located in Westerly, Rhode Island and accessible as of 2 February 2023.
-- [USPER 38] located in Easley, South Carolina and accessible as of 2 February 2023.
-- [USPER 39] located in Rapid City, South Dakota and accessible, as of 2 February 2023.
-- [USPER 40] located in Chattanooga, Tennessee and inaccessible, as of 2 February 2023.
-- [USPER 41] located in Arlington, Texas and accessible, as of 2 February 2023.
-- [USPER 42] located in Midvale, Utah and accessible as of 2 February 2023.

-- [USPER 43] located in Burlington, Vermont and accessible as of 2 February 2023.
-- [USPER 44] located in Winchester, Virginia and accessible as of 2 February 2023.
-- [USPER 45] located in Washington, District of Columbia and accessible as of 2 February 2023.
-- [USPER 46] located in Morgantown, West Virginia and inaccessible as of 2 February 2023.
-- [USPER 47] located in Milwaukee, Wisconsin and accessible as of 2 February 2023.
-- [USPER 48] located in Laramie, Wyoming and accessible as of 2 February 2023.

(U//FOUO) COMMENTS:
1. (U//FOUO) Collector Comment: These attacks occurred on 31 January 2023, one day after Killnet and Anonymous Russia targeted 29 other identified American healthcare and medical institutions. For more information, see OSIR-04001-0265-23 and OSIR-04001-0248-23.

2. (U//FOUO) Collector Comment: Content was machine-translated from Russian to English.

3. (U//FOUO) Collector Comment: All time zones were converted from UTC to EST.

(U//FOUO) PREP: OSRN-061

(U//FOUO) TIP/LEAD: None

(U//FOUO) POC: Direct feedback, evaluations, comments, and follow on collection requests to the Current and Emerging Threats Center (CETC), Open Source Collection Operations (OSCO) by accessing the OSIR evaluation link at Intelink-U (https://intelshare.intelink.gov/sites/dhs-osco/), Intelink-S (https://intelshare.intelink.sgov.gov/sites/dhs-osco/), or Intelink-TS (https://intelshare.intelink.ic.gov/sites/dhs-osco/). Contact CETC OSCO at 202-447-3688 or via e-mail at: CETC.OSCO@hq.dhs.gov, CETC.OSCO@dhs.sgov.gov, or CETC.OSCO@dhs.ic.gov.

===========================DISSEMINATION==========================
(U//FOUO) AGENCY: ATF; CIA; DEA; DHS; DIA; DNI; Energy; FBI; Justice; MCIA; NASIC; NCTC; NGA; NGIC; NRO; NSA; ONI; State; Treasury; USAFRICOM; USCENTCOM; USCYBERCOM; USEUCOM; USMS; USNORTHCOM; USPACOM; USSF; USSOCOM; USSOUTHCOM; USSTRATCOM; USTRANSCOM

(U//FOUO) DHS COMPONENTS: CBP; CIS; CISA; FEMA; ICE; TSA; USCG; USSS

(U//FOUO) STATE/LOCAL: All Field Ops

(U//FOUO) ATTACHMENTS: See attached.

---------------------------BEGIN TEARLINE----------------------------

UNCLASSIFIED//REL TO USA, FVEY

(U) WARNING: The following information is releasable to the governments of Australia, Canada, United Kingdom, and New Zealand. It may be discussed with appropriately cleared members of the Australian, Canadian, British, and New Zealand governments who have a need to know this information in accordance with their official duties. Further dissemination to other countries is not authorized without prior approval of the originator.

(U) SERIAL: 04001-0270-23

(U//REL USA, FVEY) Pro-Russian hacker group, Killnet, announced an "L7" distributed denial of service (DDoS) attack on "50 hospitals" across "50 states of America". The announcement included a list of domains and subdomains of healthcare and medical institutions located across 47 U.S. states and the District of Columbia. As of 2 February 2023, 41 of the 48 targeted domains and subdomains were accessible.

(U) INTELLIGENCE PURPOSES ONLY: This information is provided only for intelligence purposes and is intended for developing potential investigative leads. It may not be used in any way that will expose intelligence sources or methods. Any attachments separated from this report are publicly available information and are not classified.

UNCLASSIFIED//REL TO USA, FVEY

-----------------------------END TEARLINE----------------------------